Research Faculty Summit 2018

Systems | Fueling future disruptions
Microcontrollers (MCUs)
low-cost, single chip computers

9 BILLION new MCU devices
built and deployed every year
Opportunity | Risk
How does a consumer know the compressor in their fridge needs to be replaced?

Option 1
Melted ice cream

Option 2
Predictive maintenance

Connected devices create profoundly better customer experiences.
What happens when you connect a device to the internet?
'When smart gadgets spy on you: Your home life is less private than you think'

"Ransomware attacks will target more IoT devices in 2018"

"Huge IoT botnet may be used for Ukraine attack"

"Industrial IoT to equip new era of corporate intruders coming in through devices"

"Hacking these IoT baby monitors is child’s play, researchers reveal"

"Security experts warn of dangers of connected home devices"

"Your smart fridge may kill you: The dark side of IoT"

"Hacking critical infrastructure via a vending machine? The IOT reality"

"The Lurking Danger of Medical Device Hackers"

"Protecting Your Family: The Internet of Things Gives Hackers Creepy New Options"

"Why the KRACK Wi-Fi mess will take decades to clean up"
Mirai Botnet attack

Everyday devices are used to launch an attack that takes down the internet for a day

100k devices

Exploited a well known weakness

No early detection, no remote update
Hackers attack casino

Attackers gain access to casino database through fish tank

Entry point was a connected thermometer

Once in, other vulnerabilities were exploited

Gained access to high-roller database
No manufacturer wants to make insecure devices

From: Hackers  
To: Consumer  
Subject: Your Fridge

We control your fridge.  
Send us $5 in bitcoin or else...

Terrorists Ignite Thousands of House Fires with Hacked Stoves
SECURITY IS FOUNDATIONAL
It must be built in from the beginning.
The 7 properties of highly secured devices

1. Hardware Root of Trust
2. Defense in Depth
3. Small Trusted Computing Base
4. Dynamic Compartments
5. Certificate-Based Authentication
6. Failure Reporting
7. Renewable Security

https://aka.ms/7properties
Some properties depend only on hardware support

Hardware Root of Trust

Unforgeable cryptographic keys generated and protected by hardware

• Hardware to protect Device Identity
• Hardware to Secure Boot
• Hardware to attest System Integrity
Some properties depend on hardware and software

Dynamic Compartments

Internal barriers limit the reach of any single failure

- Hardware to Create Barriers
- Software to Create Compartments
Some properties depend on hardware, software and cloud

Renewable Security

Device security renewed to overcome evolving threats

- Cloud to **Provide Updates**
- Software to **Apply Updates**
- Hardware to **Prevent Rollbacks**
Azure Sphere is an end-to-end solution for securing MCU powered devices.
Azure Sphere Certified MCUs from silicon partners, with built-in Microsoft security technology provide connectivity and a dependable hardware root of trust.
The Azure Sphere OS
secured by Microsoft for the devices 10-year lifetime to create a trustworthy platform for new IoT experiences
The Azure Sphere Security Service guards every Azure Sphere device; it brokers trust for device-to-device and device-to-cloud communication, detects emerging threats, and renews device security.
Azure Sphere certified MCUs create a secured root of trust for connected, intelligence edge devices

**CONNECTED** with built-in networking

**SECURED** with built-in Microsoft silicon security technology including the Pluton Security Subsystem

**CROSSOVER** Cortex-A processing power brought to MCUs for the first time
Pluton: A bodyguard for your device

Pluton is the hardware root of trust in an Azure Sphere device.
Pluton: A bodyguard for your device

Pluton guarantees the authenticity of your software.
Pluton: A bodyguard for your device

Pluton protects against downgrade attacks.
Pluton guarantees the authenticity of your device.
Pluton: A bodyguard for your device

Pluton reduces supply chain risk.
Pluton accelerates cryptographic tasks.

Pluton: A bodyguard for your device
Pluton: A bodyguard for your device

Pluton protects against low entropy attacks.
Azure Sphere MCU’s create a secured foundation for intelligent edge devices

Pluton features implemented in silicon include:

A hardware root of trust that
- accelerates common cryptographic operations (ECC and AES)
- generates public/private keypairs
- implements secure boot (via ECDSA)

A dedicated core and memory (TCM) that
- resists side-channel attacks that focus on a single core

A true random number generator that
- defends against low-entropy attacks

Measured boot and remote attestation that
- uses a digest accumulator register and nonce register
Cortex-A:

- Multiplexed I/O
  - SPI
  - I2C
  - UART
  - I2S
  - TDM
  - PWM
  - GPIO
  - ADC

ARM Cortex-A
- optimized for low power

Flash
- ≥ 4MB

Network Connection
- WiFi in first chips

Microsoft Pluton
- Security Subsystem

SRAM
- ≥ 4MB

ARM Cortex-M
- for real-time processing

Firewall

Multiplexed I/O
- GPIO
- PWM
- TDM
- I2S
- UART
- I2C
- SPI
- ADC
Cortex-A:

SECURITY

- Multiplexed I/O
- SPI
- I2C
- UART
- I2S
- TDM
- PWM
- GPIO
- ADC

ARM Cortex-A
optimized for low power

Microsoft Pluton
Security Subsystem

FLASH ≥ 4MB

Network Connection
WiFi in first chips

SRAM ≥ 4MB

ARM Cortex-M
for real time processing

Firewall

Multiplexed I/O

GPIO, PWM, TDM, I2S, UART, I2C, SPI, ADC
Cortex-A:

SECURITY

PORTABILITY
Cortex-A:

SECURITY

PORTABILITY

EXTENSIBILITY
Isolation

The Cortex-A provides process-level isolation via its Memory Management Unit (MMU). The Azure Sphere IoT OS leverages the MMU as part of the application container to protect other applications and services.
Specialized operating system

The Azure Sphere OS includes the Azure Sphere runtime and a custom Linux kernel with special IoT functionality. Example: Azure Sphere OS reduces its attack surface by not using passwords, a shell or login. All benefits of a Linux kernel without wasted overhead.
Authentication

Azure Sphere OS uses client and server certificate authentication for cloud communication.
Authorization

Azure Sphere OS authorizes access to resources via a custom capability system secured by Pluton.
Accelerated time to market

MMU provides address-space virtualization. Azure Sphere OS provides hardware abstraction. Application code is written once and portable across Azure Sphere chips.
Source portability

Open source software (OSS) libraries are often written against the POSIX standard. Azure Sphere OS includes a large subset of the POSIX standard, allowing rapid porting of OSS software to your application platform.
A7 headroom for the future

Machine learning, machine translation, vision and AI will be the future of many products. The Cortex-A has headroom for new product features and customer experiences that will set your products apart.
A secure foundation in silicon

Microsoft firewalls implement the principle of least-privilege. Software behind the firewall is given access to only those resources that it is given explicit permission.
Comprehensive protection

This principle applies to every resource in the system: RAM, network, flash and peripherals.
Hackers have no way out

Compromised software cannot access new resources.
Sticky from the start

Further, firewalls are sticky. Even if the layer that controls the firewall is compromised, it is not possible to reconfigure until the chip is reset.
Real-time computation

MCUs targeted at real-time computation and real-time interaction with peripherals.
Low-friction migration

Azure Sphere MCUs provide Cortex-M series MCUs to run your existing MCU collateral secured by Pluton.
Maximum flexibility

Manufacturers are free to run any Cortex-M runtime.

Microsoft will provide a reference M4 runtime.
Our Silicon Partners

- MediaTek
- ARM
- STMicroelectronics
- NXP
- Silicon Labs
- Nordic
- Nuvoton
- Hilscher
- Toshiba
- VeriSilicon
- Qualcomm
The Azure Sphere OS is optimized for IoT, security, and agility

**Secure Application Containers**
Compartmentalize code for agility, robustness & security

**On-chip Cloud Services**
Provide update, authentication, and connectivity

**Custom Linux kernel**
Empowers agile silicon evolution and reuse of code

**Security Monitor**
Guards integrity and access to critical resources

### Azure Sphere OS Architecture

<table>
<thead>
<tr>
<th>OS Layer 4</th>
<th>App Containers for POSIX (on Cortex-A)</th>
<th>App Containers for I/O (on Cortex-Ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Layer 3</td>
<td>On-chip Cloud Services</td>
<td></td>
</tr>
<tr>
<td>OS Layer 2</td>
<td>HLOS Kernel</td>
<td></td>
</tr>
<tr>
<td>OS Layer 1</td>
<td>Security Monitor</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Azure Sphere MCUs</td>
<td></td>
</tr>
</tbody>
</table>
Curated user-mode environment
e.g., no passwords, no shell, no user accounts
Azure Sphere application runtime provides long-term compatibility with OS

OS Services manage connectivity & chip resources
e.g., TLS connection, mutual authentication, peripheral access

Custom Linux Kernel
Linux Security Module protects resource acquisition
Kernel integrates with Pluton services (e.g., RNG)

Security monitor protects critical resources
Guards against corruption using a technique called “erasure coding”
Boot health-check detects and self-heals corrupted data

---

### Azure Sphere OS Architecture

<table>
<thead>
<tr>
<th>OS Layer 4</th>
<th>App Containers for POSIX (on Cortex-A)</th>
<th>App Containers for I/O (on Cortex-Ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Layer 3</td>
<td>On-chip Cloud Services</td>
<td></td>
</tr>
<tr>
<td>OS Layer 2</td>
<td>HLOS Kernel</td>
<td></td>
</tr>
<tr>
<td>OS Layer 1</td>
<td>Security Monitor</td>
<td></td>
</tr>
</tbody>
</table>

Hardware: Azure Sphere MCUs
Protects your devices and your customers with certificate-based authentication of all communication

Detects emerging security threats through automated processing of on-device failures

Responds to threats with fully automated on-device updates of OS

Allows for easy deployment of software updates to Azure Sphere powered devices
Azure Sphere online services in action

Using attestation to control access to online services

Up-to-date devices are issued a short-lived certificate

Any service that can validate the cert chain can verify attestation completed successfully

Out-of-date devices may be forced to update
Modernize MCU development with Azure Sphere and Visual Studio

Simplify development
Focus your device development effort on the value you want to create

Streamline debugging
Experience interactive, context-aware debugging across device and cloud

Collaborate across your team
Apply tool-assisted collaboration across your entire development organization
Three components. One low price. No subscription required.

An Azure Sphere certified MCU

The Azure Sphere OS with 10 years of on-device security updates

The Azure Sphere Security Service for the lifetime of your device
Azure Sphere is Open.

Open to any MCU manufacturer
We are licensing our Pluton security subsystem royalty **free for use** in any chip*

Open to any innovation
MCU manufacturers are free to innovate with our GPL’d OSS Linux kernel code base

Open to any cloud
Azure Sphere devices are free to connect to Azure or any other cloud, proprietary or public for application data
Let’s secure the future.
Thank you!